DES

Cifras de Bloco

Prof. Dr. Iaçanã Ianiski Weber

Confiabilidade e Segurança de Software

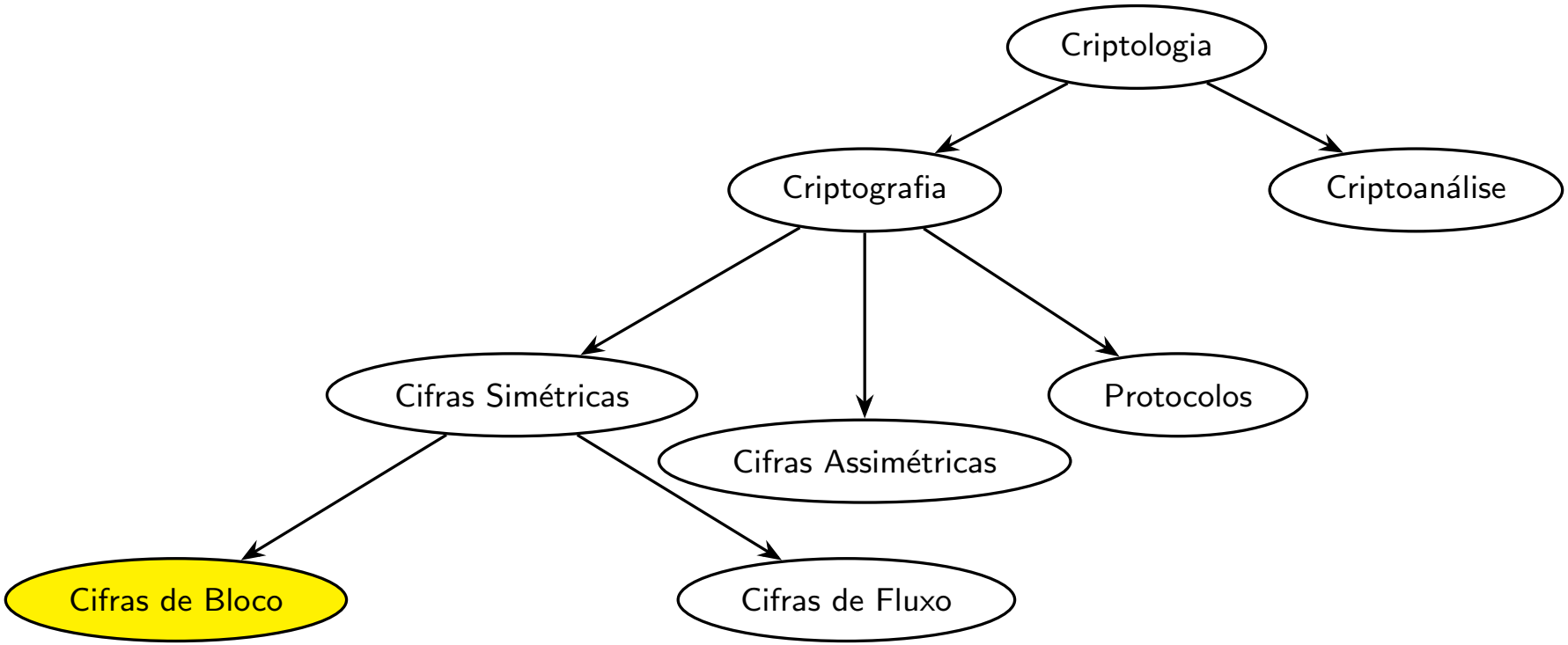
98G08-4

Agradecimentos especiais ao Prof. Avelino Zorzo e aos Autores Christof Paar e Jan Pelzl pelo material.

Índice

Índice

DES no campo da Criptologia



Fatos sobre o DES

- **Data Encryption Standard (DES)** cifra blocos de tamanho **64 bits**.
- Desenvolvido pela **IBM** com base na cifra *Lucifer*, sob influência da **National Security Agency (NSA)**.
- Os critérios de projeto do DES nunca foram publicados.
- **Padronizado em 1977** pelo **National Bureau of Standards (NBS)**, hoje chamado de **National Institute of Standards and Technology (NIST)**.
- Foi a cifra de bloco mais popular durante cerca de 30 anos.
- É o algoritmo simétrico mais estudado até hoje.
- Atualmente é considerado inseguro devido ao pequeno **tamanho de chave: 56 bits**.
- **3DES foi uma evolução que foi considerada segura** até 2019.
- Foi substituído em 2000 pelo **Advanced Encryption Standard (AES)**.

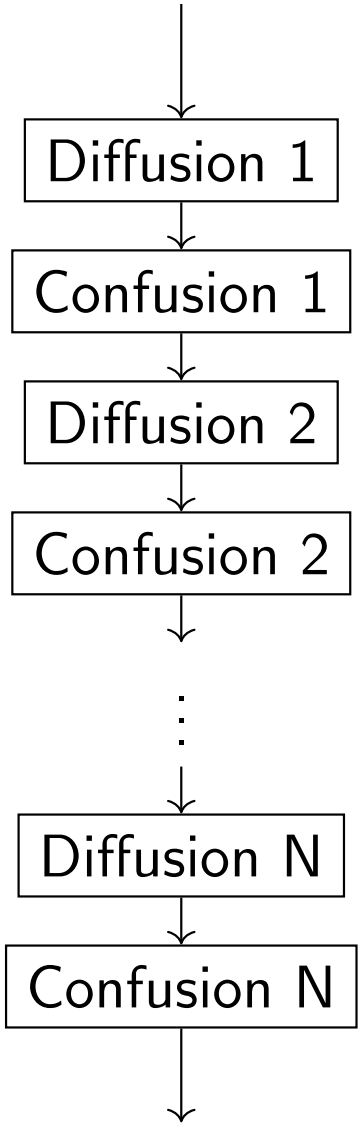
Primitivas de Cifras em Bloco: Confusão e Difusão

- Claude Shannon identificou duas operações primitivas a partir das quais algoritmos de criptografia fortes podem ser construídos:

- **1. Confusão:** Uma operação de criptografia na qual a **relação entre a chave e o ciphertext é obscurecida**.
  Hoje, um elemento comum para atingir a confusão é a **substituição**, encontrada tanto no AES quanto no DES.

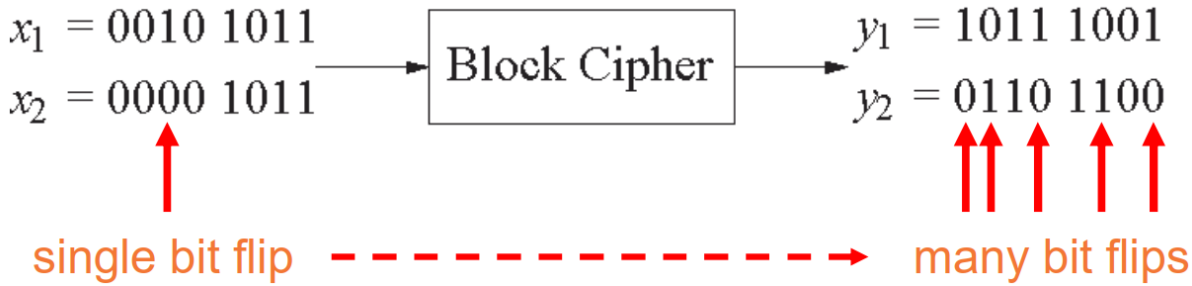
- **2. Difusão:** Uma operação de criptografia na qual a **influência de um símbolo do plaintext se espalha por muitos símbolos do ciphertext**, com o objetivo de esconder propriedades estatísticas do plaintext.
  Um exemplo simples de difusão é a **permutação de bits**, amplamente utilizada no DES.

Cifras de Produto



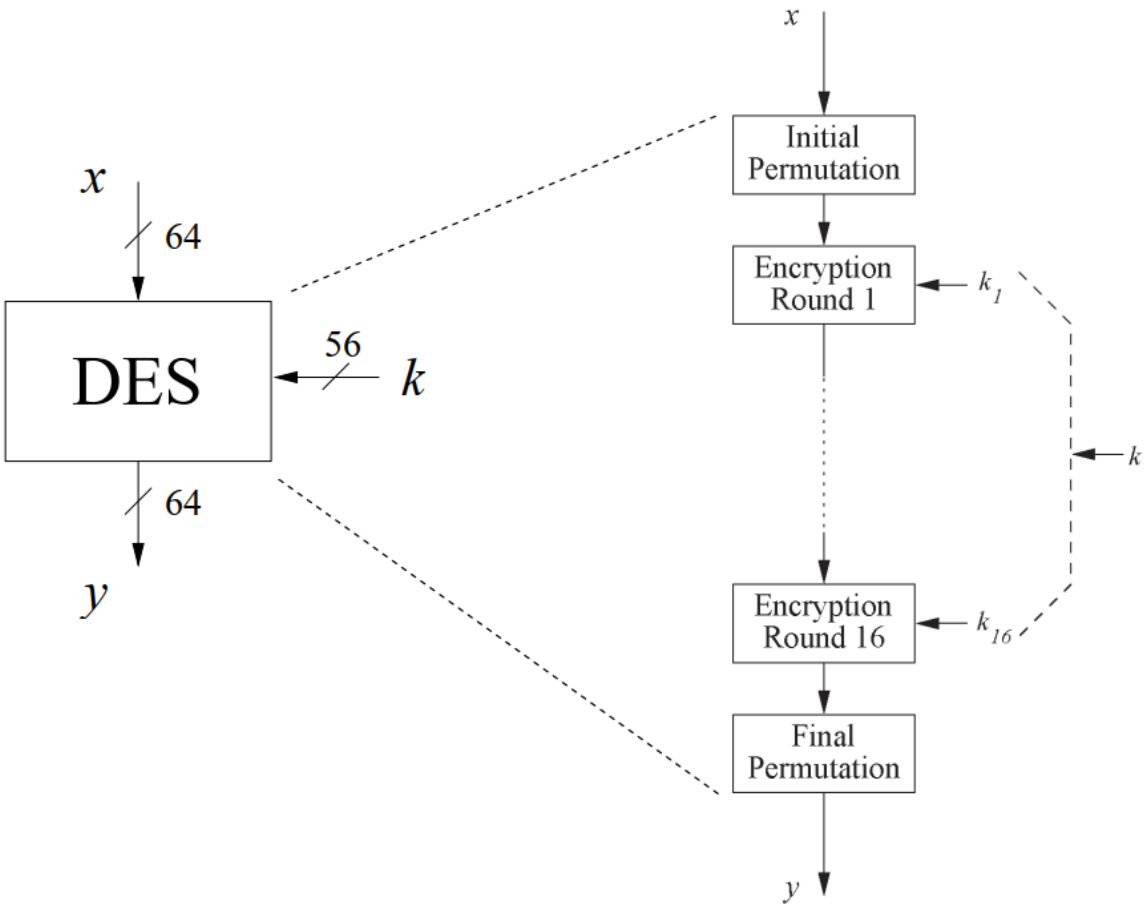
- A maioria das cifras de bloco modernas são compostas por rodadas repetidas de confusão e difusão.
- Podem alcançar excelente difusão: *alterar um único bit do plaintext muda, em média, metade dos bits de saída*.

Exemplo:



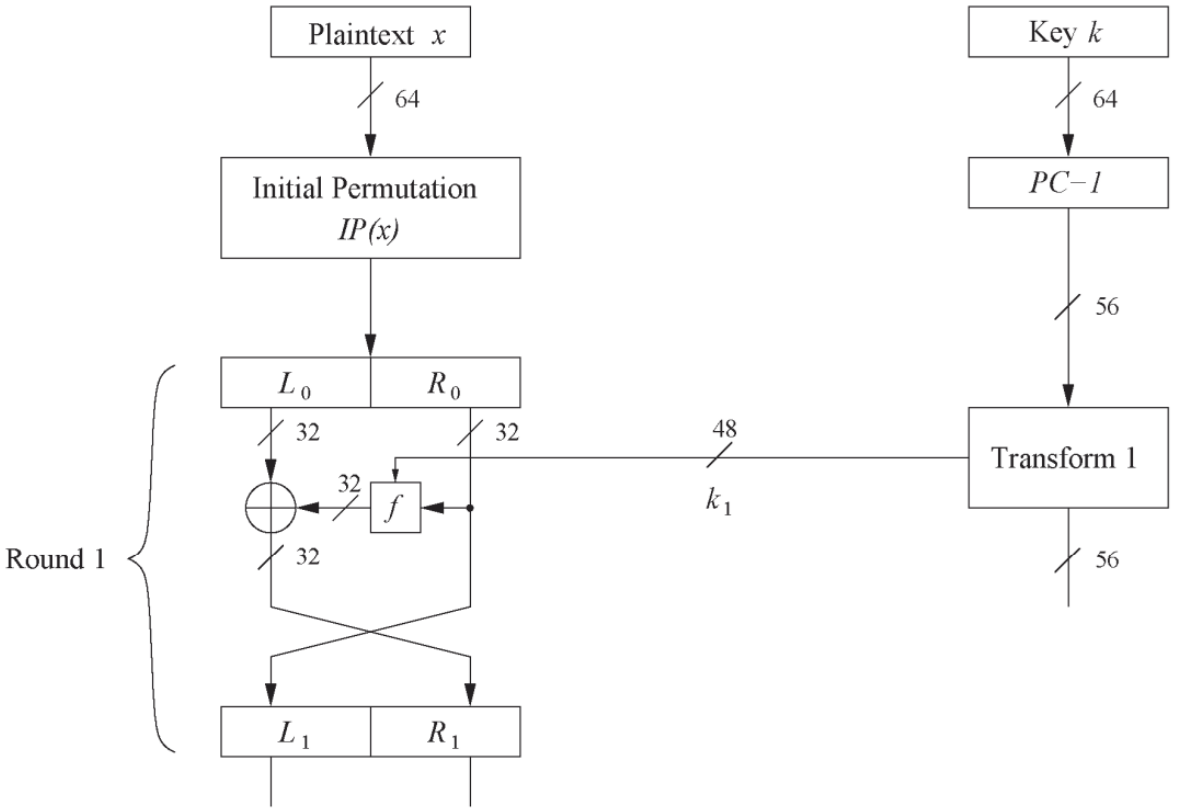
Índice

Visão Geral do Algoritmo DES



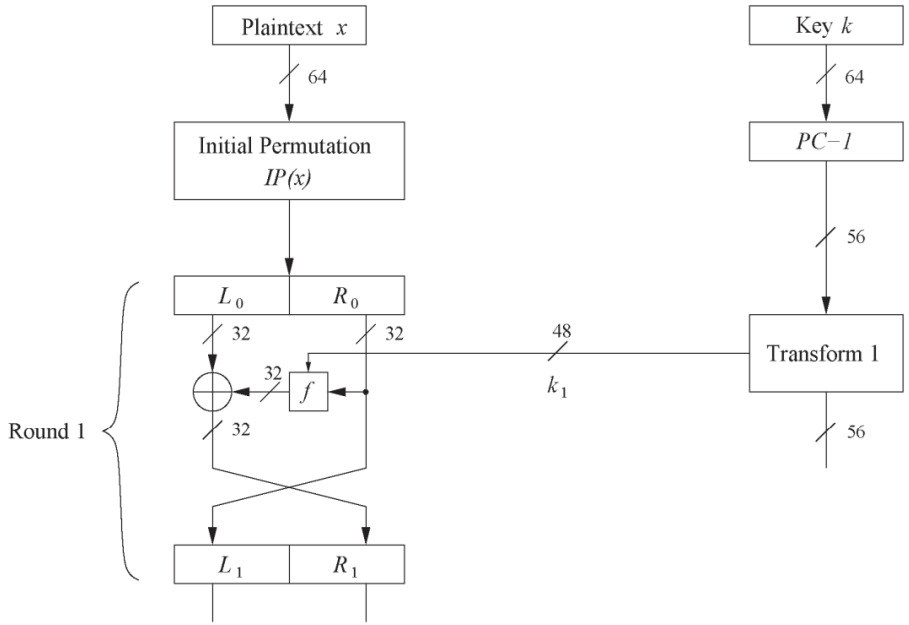
- **Cifra de Bloco:** cifra blocos de 64 bits.
- **Chave de 56 bits.**
- **Cifra simétrica**: mesma chave para cifrar e decifrar.
- Utiliza 16 rodadas idênticas de transformação.
- Em cada rodada, é utilizada uma subchave (chave da rodada) derivada da chave principal.

Rede Feistel do DES (1)



- A estrutura do DES é uma *rede Feistel*.
- Vantagem: cifragem e decifragem diferem apenas na geração das chaves da rodada.
- Permutação inicial bit a bit, seguida de 16 rodadas.

Rede Feistel do DES (2)



Etapas por rodada:

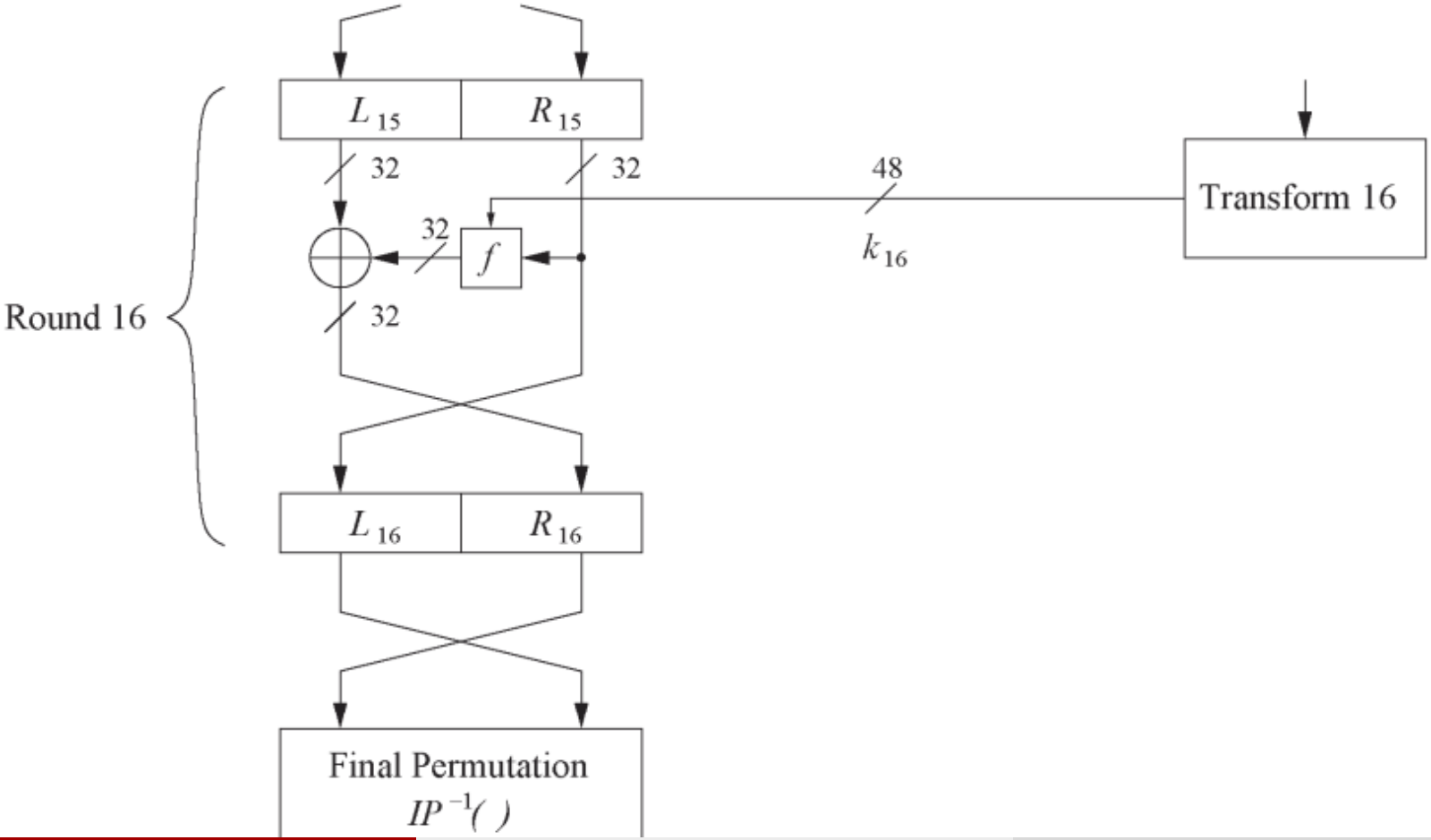
1. Divide-se o *plaintext* em duas metades de 32 bits: L_i e R_i
2. R_i entra na função f, cujo resultado é combinado com L_i via XOR
3. As metades esquerda e direita são trocadas

Expressão das rodadas:

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

Rede Feistel do DES (3)

- No final da cifra, as metades L e R são trocadas novamente
- Isso ocorre após a 16ª rodada da função Feistel
- Em seguida, aplica-se a **Permutação Final** IP^{-1}
- O resultado é o **ciphertext final** $y = \mathrm{DES}_k(x)$



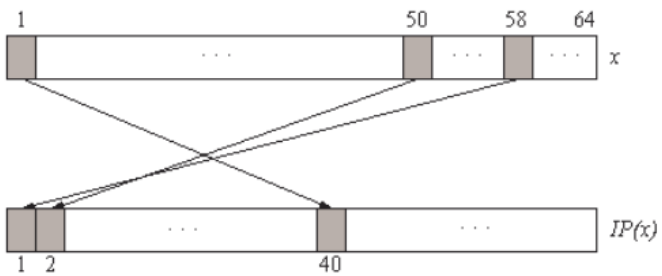
Índice

Permutação Inicial e Final

- Permutações bit a bit aplicadas sobre o bloco de entrada.
- Operações inversas entre si.
- Definidas pelas tabelas IP e IP^{-1}.

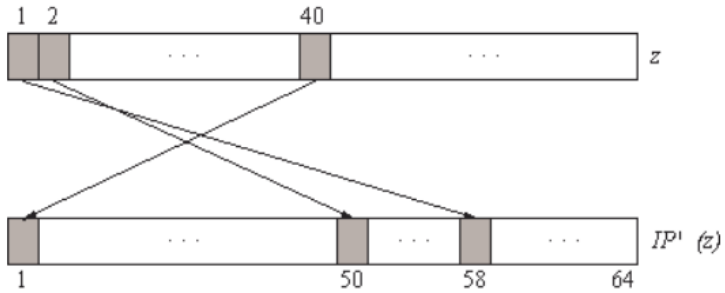
Initial Permutation

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7



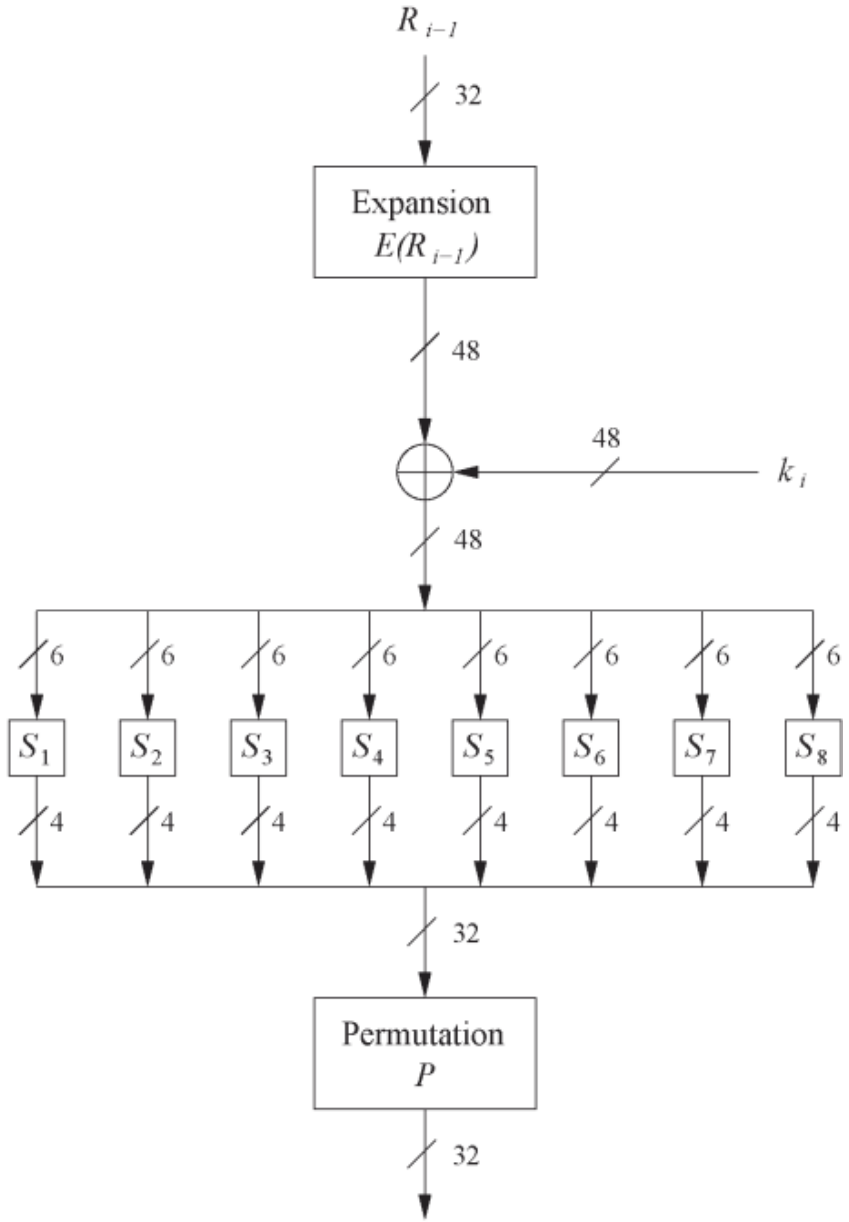
Final Permutation

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



A função f do DES

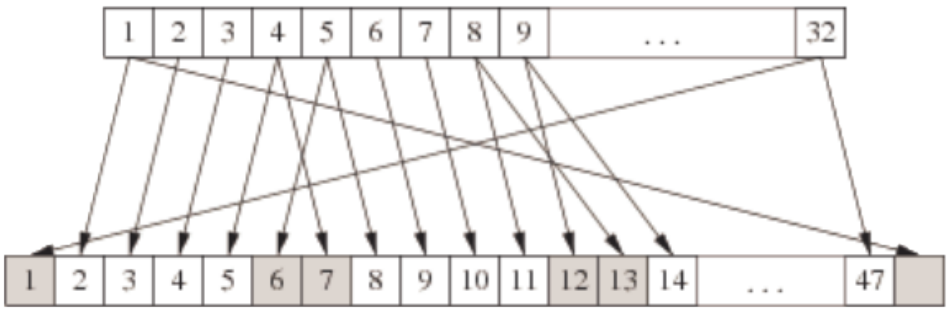
- **Operação principal** do algoritmo DES.
- Entradas da função f: R_{i-1} e a chave da rodada k_i.
- **4 etapas:**
  1. Expansão E
  2. Operação XOR com a chave de rodada
  3. Substituição via caixas-S (*S-boxes*)
  4. Permutação P

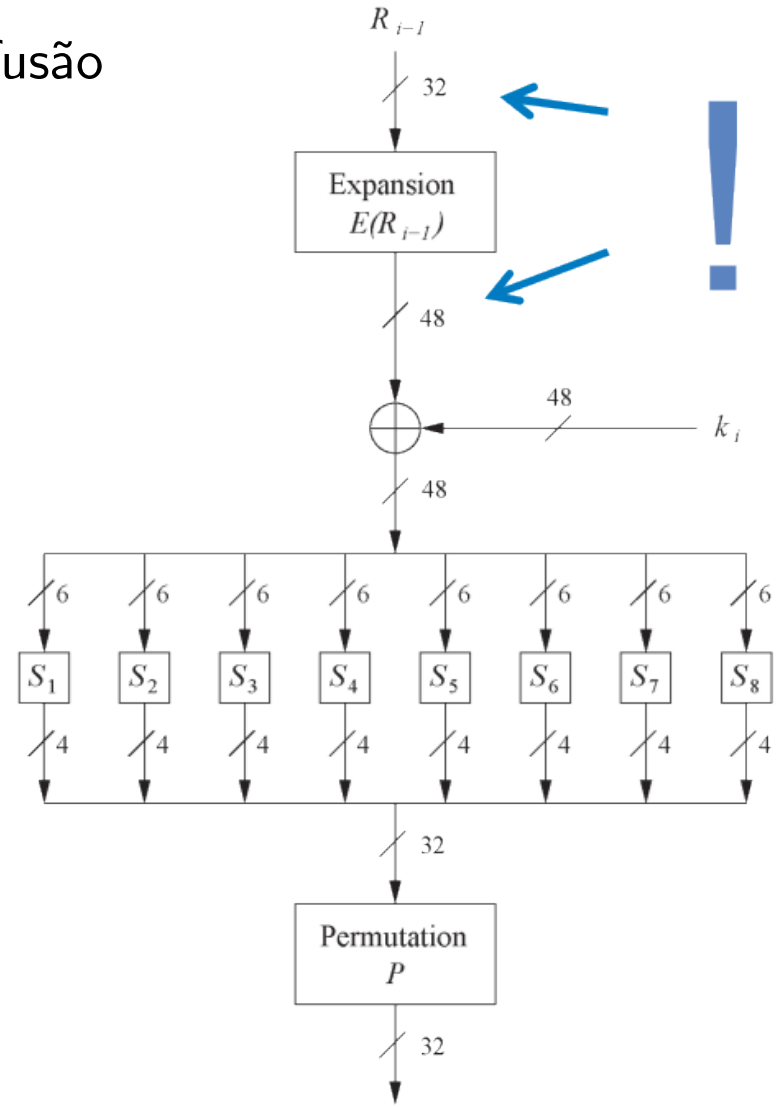


Função de Expansão E

- **1. Expansão E**
  - **Objetivo principal:** aumentar a difusão

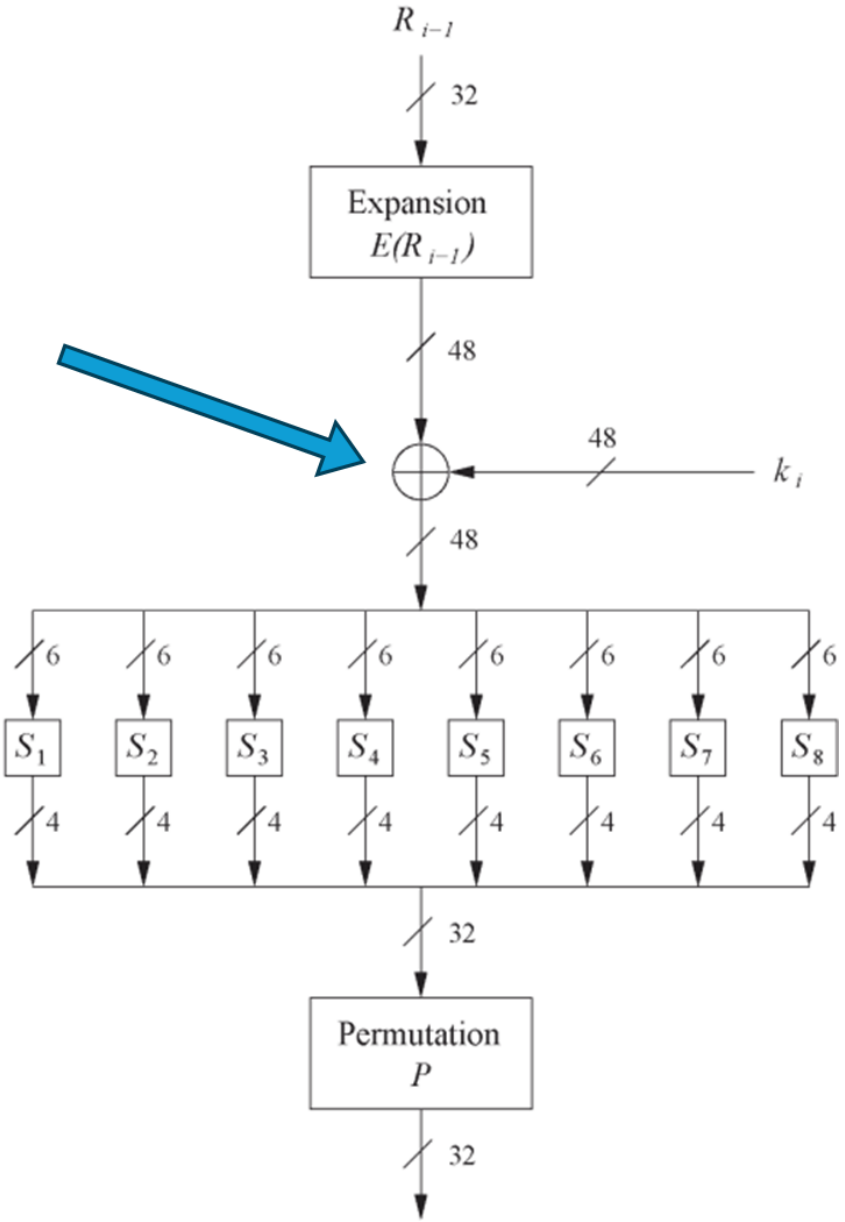
E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1





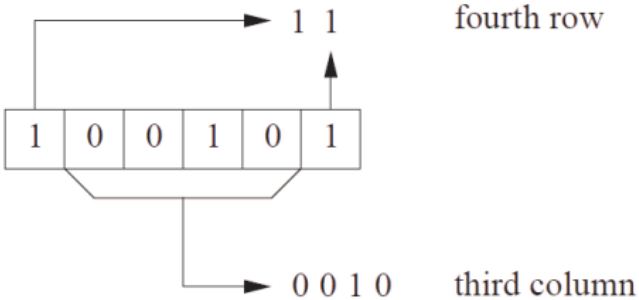
Adicionar Chave da Rodada

2. **XOR com a Chave da Rodada**
   - XOR bit a bit da chave da rodada com a saída da função de expansão E.
   - As chaves de rodada são derivadas da chave principal no processo de geração de chaves do DES (será mostrado em alguns slides).

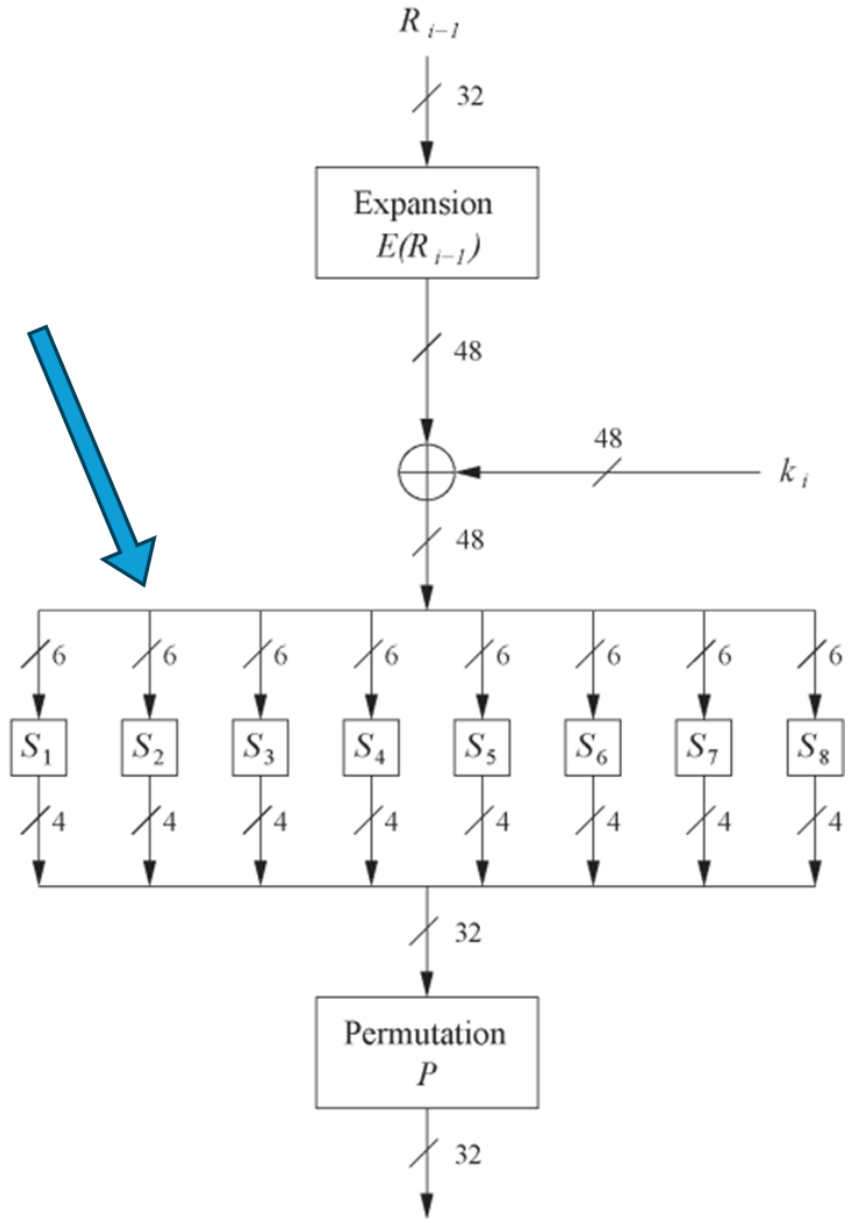


As S-Boxes do DES

3. **Substituição S-Box**
   - Oito tabelas de substituição.
   - 6 bits de entrada, 4 bits de saída.
   - Não-linear e resistente à criptoanálise diferencial.
   - Elemento crucial para a segurança do DES!



S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

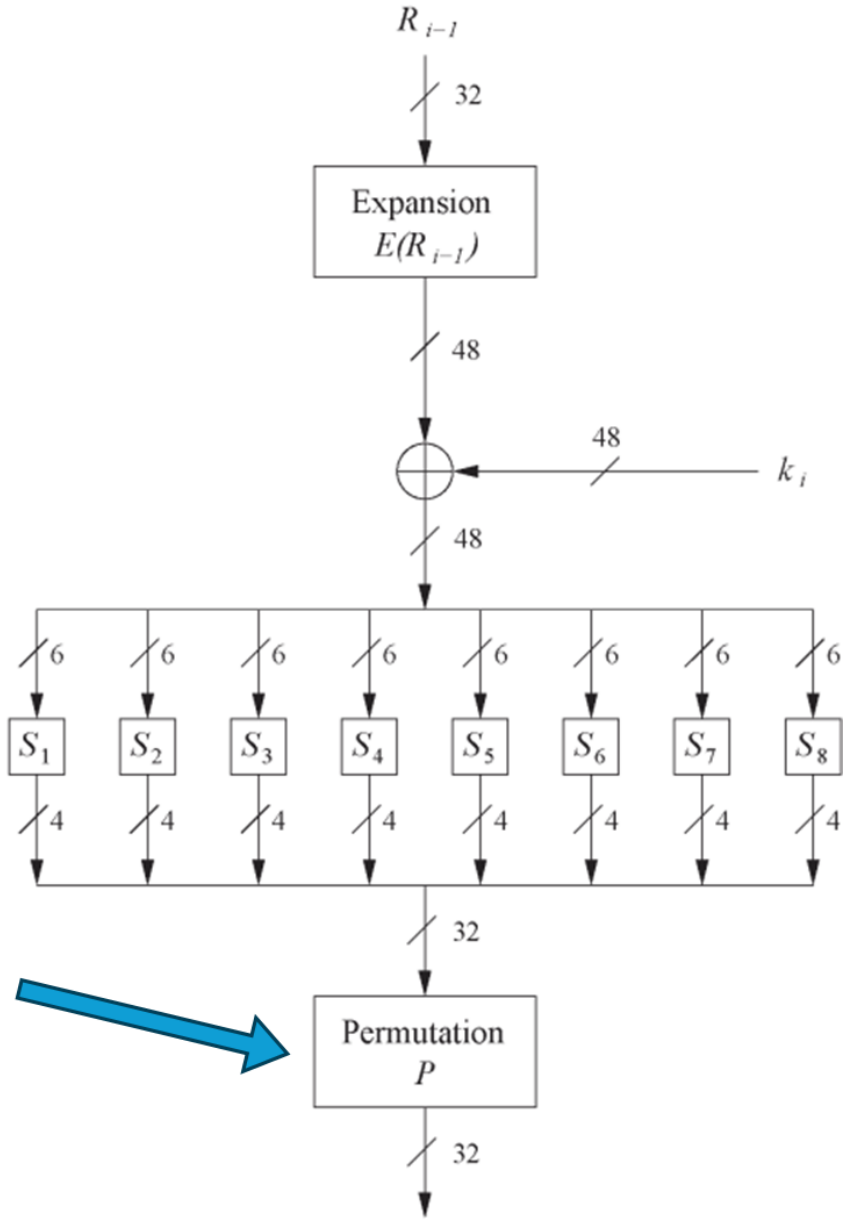


A permutação P

4. **Permutação P**

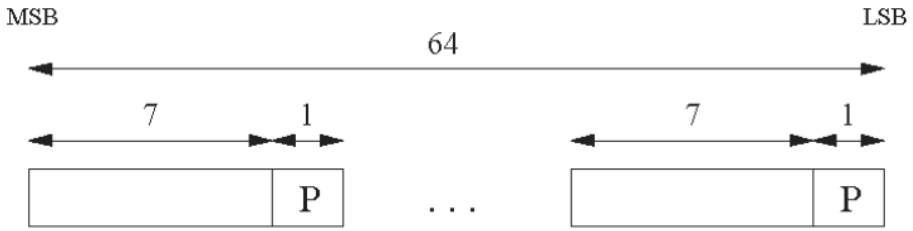
- Permutação bit a bit.
- Introduz difusão.
- Os bits de saída de uma S-Box afetam várias S-Boxes na próxima rodada.
- A difusão pelas funções E, S-Boxes e P garante que, após a quinta rodada, cada bit depende de cada bit da chave e de cada bit do texto claro.

P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25



Chave da Rodada (1)

- Deriva 16 chaves de rodada (ou *subchaves*) k_i de 48 bits cada a partir da chave original de 56 bits.
- O tamanho da chave de entrada do DES é de 64 bits: **56 bits de chave** e 8 bits de paridade:



P = parity bit

- **Os bits de paridade são removidos** na primeira permutação $PC-1$: 8, 16, 24, 32, 40, 48, 56 e 64 não são usados.

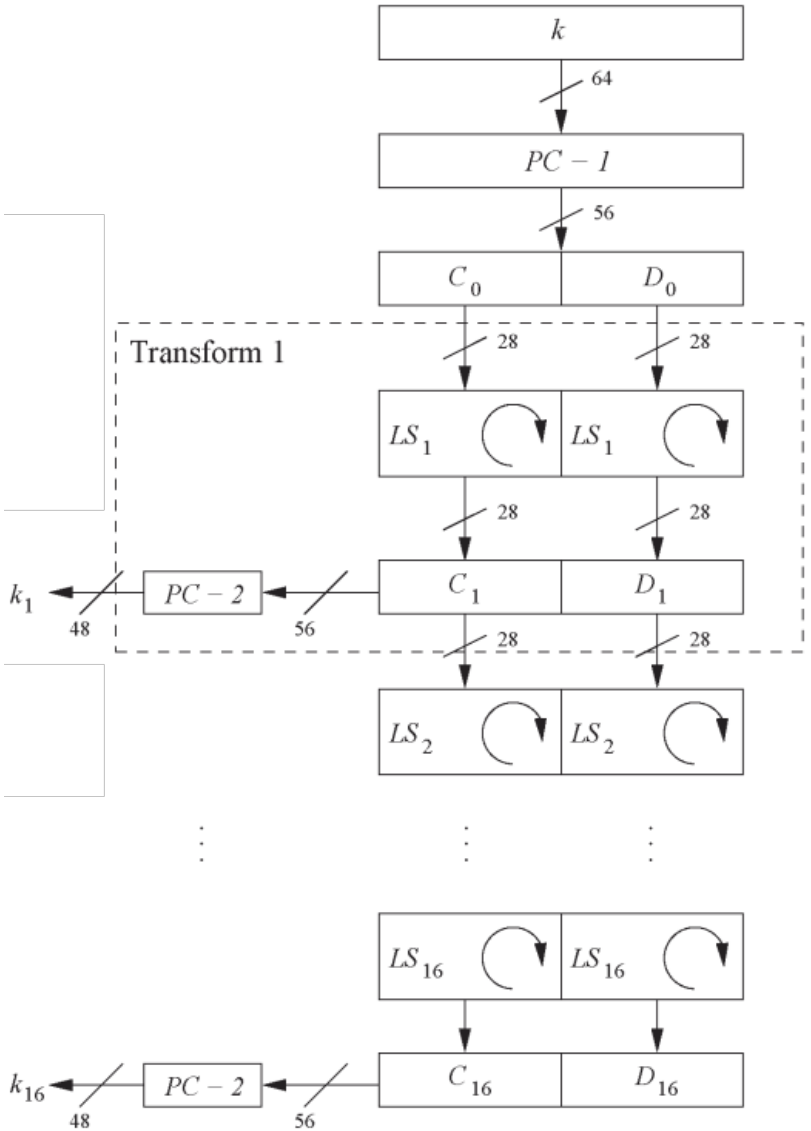
PC-1							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	28	20	12	4
61	53	45	37	29	21	13	5
62	54	46	38	30	22	14	6
63	55	47	39	31	23	15	7

Chave da Rodada (2)

- Divide a chave em metades de 28 bits C_0 e D_0.
- Nas rodadas $i = 1, 2, 9, 16$, as duas metades são rotacionadas à esquerda por **um bit**.
- Em todas as outras rodadas, as duas metades são rotacionadas à esquerda por **dois bits**.
- *Em cada rodada* i, a escolha permutada $PC-2$ seleciona um subconjunto permutado de 48 bits de C_i e D_i como chave da rodada k_i, ou seja, **cada** k_i **é uma permutação de** k**!**

PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

- **Nota:** O número total de rotações:
  $4 \times 1 + 12 \times 2 = 28 \quad \Rightarrow \quad D_0 = D_{16}, C_0 = C_{16}!$



Índice

Descriptografia

- Em cifras que usam a Rede de *Feistel*, apenas a geração da chave da rodada precisa ser modificada para a descriptografia.
- Gerar as mesmas 16 chaves de rodada, mas em ordem inversa.

- **Agendamento de chaves invertido:**
  Como $D_0 = D_{16}$ e $C_0 = C_{16}$, a primeira chave de rodada pode ser gerada aplicando $PC-2$ logo após $PC-1$ (sem rotação aqui!).
- Todas as outras rotações de C e D podem ser revertidas para reproduzir as demais chaves de rodada, resultando em:
  - Nenhuma rotação na rodada 1.
  - Uma rotação de 1 bit para a direita nas rodadas 2, 9 e 16.
  - Duas rotações de 2 bits para a direita em todas as outras rodadas.

Índice

Segurança do DES

- **Após a proposta do DES, surgiram duas críticas principais:**
  1. O espaço de chaves é muito pequeno (2^{56} chaves).
  2. Os critérios de projeto das S-Boxes foram mantidos em segredo: haveria algum ataque analítico oculto (*backdoors*), conhecido apenas pela NSA?
- **Ataques Analíticos:** O DES é altamente resistente tanto à *criptoanálise diferencial* quanto à *criptoanálise linear*, publicadas anos depois do DES.
  - Isso indica que a IBM e a NSA já conheciam esses ataques 15 anos antes!
  - Até hoje, não há ataque analítico conhecido que quebre o DES em cenários realistas.
- **Busca exaustiva de chaves:** Dado um par texto-claro/texto-cifrado (x, y), testa-se todas as 2^{56} chaves até encontrar $DES_k^{-1}(x) = y$.
  $\Rightarrow$ Relativamente fácil com a tecnologia computacional atual!

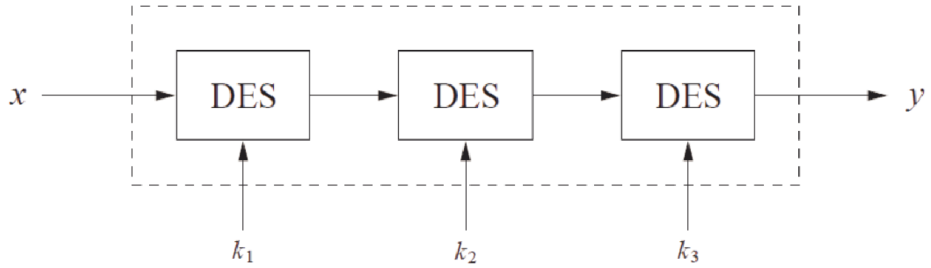
Histórico de Ataques ao DES

Ano	Ataque Proposto/Implementado ao DES
1977	Diffie & Hellman estimam (subestimam) os custos de uma máquina de busca por chave
1990	Biham & Shamir propõem a criptoanálise diferencial (2^{47} textos-cifrados escolhidos)
1993	Mike Wiener propõe o design de uma máquina de busca por chave muito eficiente: busca média requer 36h. Custo: \$1.000.000
1993	Matsui propõe a criptoanálise linear (2^{43} textos-cifrados escolhidos)
Jun. 1997	DES Challenge I quebrado em 4,5 meses de busca distribuída
Fev. 1998	DES Challenge II–1 quebrado em 39 dias (busca distribuída)
Jul. 1998	DES Challenge II–2 quebrado, máquina de busca por chave *Deep Crack* construída pela Electronic Frontier Foundation (EFF): 1800 ASICs com 24 motores de busca cada; Custo: \$250.000, média de busca: 15 dias (levou 56h no desafio)
Jan. 1999	DES Challenge III quebrado em 22h 15min (busca distribuída assistida por *Deep Crack*)
2006–2008	Máquina reconfigurável de busca por chave *COPACOBANA* desenvolvida nas Universidades de Bochum e Kiel (Alemanha), usa 120 FPGAs para quebrar o DES em 6,4 dias (média) com custo de \$10.000

Triple DES – 3DES

- A cifra *triple-DES* é frequentemente utilizada na prática para estender o comprimento efetivo da chave do DES para 112 bits.

$$y = DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$$



- Versão alternativa do **3DES:** $y = DES_{k_3}(DES^{-1}_{k_2}(DES_{k_1}(x)))$
- Vantagem: escolher $k_1 = k_2 = k_3$ equivale a realizar uma única cifragem DES.
- Usado em muitas aplicações legadas, por exemplo, em sistemas bancários.
- O NIST baniu o uso do 3DES para novos sistemas a partir de 2017.
- AES substituiu o 3DES na maioria dos sistemas modernos.

Alternativas ao DES

Algoritmo	**I/O (bits)**	**Tamanho da chave (bits)**	**Observações**
AES / Rijndael	128	128/192/256	Substituto oficial do DES (padrão NIST)
Triple DES	64	112 (efetivo)	Uso desaconselhado pelo NIST (*deprecated*)
ChaCha20	512	256	Utilizado em TLS 1.3, Google, OpenSSH
Mars	128	128/192/256	Finalista do AES
RC6	128	128/192/256	Finalista do AES
Serpent	128	128/192/256	Finalista do AES
Twofish	128	128/192/256	Finalista do AES
IDEA	64	128	Algoritmo patenteado
Camellia	128	128/192/256	Padrão ISO/IEC, amplamente usado na Ásia

Lições Aprendidas

- O DES foi o algoritmo de criptografia simétrica dominante de meados da década de 1970 até meados da década de 1990. Como as chaves de 56 bits não são mais seguras, foi definido o *Advanced Encryption Standard* (AES).
- O DES padrão, com chave de 56 bits, pode ser quebrado relativamente fácil hoje em dia por meio de uma busca exaustiva de chaves.
- O DES é bastante robusto contra ataques analíticos conhecidos: na prática, é muito difícil quebrar o cifrador usando criptoanálise diferencial ou linear.
- Ao cifrar com o DES três vezes consecutivas, cria-se o Triple DES (3DES), que possui uma segurança maior.
- O cifrador simétrico "padrão" atualmente é geralmente o AES. Além disso, os outros quatro finalistas do AES também são considerados muito seguros e eficientes.

Índice

Exercício: Não-linearidade das S-Boxes

Conforme apresentado, uma propriedade importante que garante a segurança do DES é que as S-Boxes são não-lineares. Neste exercício, verificamos essa propriedade computando a saída da S_1 para alguns pares de entradas.
Mostre que:

$$S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$$

onde "$\oplus$"denota o XOR bit a bit, para os seguintes casos:

1. $x_1 = 000000,\ x_2 = 000001$
2. $x_1 = 111111,\ x_2 = 100000$
3. $x_1 = 101010,\ x_2 = 010101$

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S-BOX S_1

Exercícios: Primeira Rodada do DES

1. Qual é a saída da **primeira rodada** do algoritmo DES quando o texto claro e a chave são ambos compostos apenas por zeros?

2. Qual é a saída da **primeira rodada** do algoritmo DES quando o texto claro e a chave são ambos compostos apenas por uns?

Dica: considere o efeito das permutações iniciais, expansão, XOR com a chave e as S-Boxes.